FEE TRANSMITTAL
For FY 2008

Effective on 12/08/2004.
Fees pursuant to the Consolidated Appropriations Act, 2005 (H.R. 4818).

Complete if Known	
Application Number	10/082,186-Conf. #4346
Filing Date	February 26, 2002
First Named Inventor	Akira Kimura
Examiner Name	M. J. Pyzocha
Art Unit	2137
Attorney Docket No.	SON-2356

[ ] Applicant claims small entity status. See 37 CFR 1.27

TOTAL AMOUNT OF PAYMENT ($) 510.00

METHOD OF PAYMENT (check all that apply)

[ ] Check [ ] Credit Card [ ] Money Order [ ] None [ ] Other (please identify): _____

[x] Deposit Account ·Deposit Account Number:____18-0013____ Deposit Account Name: Rader, Fishman & Grauer PLLC

For the above-identified deposit account, the Director is hereby authorized to: (check all that apply)

[x] Charge fee(s) indicated below

[ ] Charge fee(s) indicated below, **except for the filing fee**

[x] Charge any additional fee(s) or underpayments of fee(s) under 37 CFR 1.16 and 1.17

[x] Credit any overpayments

FEE CALCULATION

1. BASIC FILING, SEARCH, AND EXAMINATION FEES

Application Type	FILING FEES Fee ($)	Small Entity Fee ($)	SEARCH FEES Fee ($)	Small Entity Fee ($)	EXAMINATION FEES Fee ($)	Small Entity Fee ($)	Fees Paid ($)
Utility	310	155	510	255	210	105	_____
Design	210	105	100	50	130	65	_____
Plant	210	105	310	155	160	80	_____
Reissue	310	155	510	255	620	310	_____
Provisional	210	105	0	0	0	0	_____

2. EXCESS CLAIM FEES

Fee Description	Fee ($)	Small Entity Fee ($)
Each claim over 20 (including Reissues)	50	25
Each independent claim over 3 (including Reissues)	200	100
Multiple dependent claims	360	180

Total Claims	Extra Claims	Fee ($)	Fee Paid ($)
_____ - _____ = _____	x _____ = _____		

HP = highest number of total claims paid for, if greater than 20.

Multiple Dependent Claims

Fee ($)	Fee Paid ($)
_____	_____

Indep. Claims	Extra Claims	Fee ($)	Fee Paid ($)
_____ - _____ = _____	x _____ = _____		

HP = highest number of independent claims paid for, if greater than 3.

3. APPLICATION SIZE FEE

If the specification and drawings exceed 100 sheets of paper (excluding electronically filed sequence or computer listings under 37 CFR 1.52(e)), the application size fee due is $260 ($130 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).

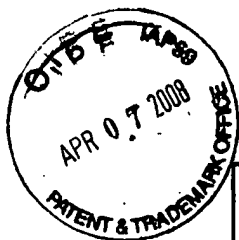| Total Sheets	Extra Sheets	Number of each additional 50 or fraction thereof	Fee ($)	Fee Paid ($)
_____ - 100 = _____	/50 = _____	(round up to a whole number) x	_____ =	_____

4. OTHER FEE(S)

Non-English Specification, $130 fee (no small entity discount)

Other (e.g., late filing surcharge): 1402 Filing a brief in support of an appeal — Fees Paid ($) 510.00

SUBMITTED BY

Signature	[signature] 44,291	Registration No. (Attorney/Agent) 24,104 / 40,290	Telephone (202) 955-3750
Name (Print/Type)	Ronald P. Kananen / Christopher M. Tobin		Date April 7, 2008

[Stamp: APR 07 2008 — PATENT & TRADEMARK OFFICE]

Effective on 12/08/2004. *Fees pursuant to the Consolidated Appropriations Act, 2005 (H.R. 4818).* # FEE TRANSMITTAL ## For FY 2008	**Complete if Known**	
	Application Number	10/082,186-Conf. #4346
	Filing Date	February 26, 2002
	First Named Inventor	Akira Kimura
	Examiner Name	M. J. Pyzocha
☐ Applicant claims small entity status. See 37 CFR 1.27	Art Unit	2137
TOTAL AMOUNT OF PAYMENT ($) 510.00	Attorney Docket No.	SON-2356

METHOD OF PAYMENT (check all that apply)

☐ Check ☐ Credit Card ☐ Money Order ☐ None ☐ Other (please identify): _____

☒ Deposit Account   Deposit Account Number: 18-0013   Deposit Account Name: Rader, Fishman & Grauer PLLC

For the above-identified deposit account, the Director is hereby authorized to: (check all that apply)

☒ Charge fee(s) indicated below   ☐ Charge fee(s) indicated below, **except for the filing fee**

☒ Charge any additional fee(s) or underpayments of fee(s) under 37 CFR 1.16 and 1.17   ☒ Credit any overpayments

FEE CALCULATION

1. BASIC FILING, SEARCH, AND EXAMINATION FEES

	FILING FEES		SEARCH FEES		EXAMINATION FEES		
Application Type	Fee ($)	Small Entity Fee ($)	Fee ($)	Small Entity Fee ($)	Fee ($)	Small Entity Fee ($)	**Fees Paid ($)**
Utility	310	155	510	255	210	105	_____
Design	210	105	100	50	130	65	_____
Plant	210	105	310	155	160	80	_____
Reissue	310	155	510	255	620	310	_____
Provisional	210	105	0	0	0	0	_____

2. EXCESS CLAIM FEES

Fee Description	Fee ($)	Small Entity Fee ($)
Each claim over 20 (including Reissues)	50	25
Each independent claim over 3 (including Reissues)	200	100
Multiple dependent claims	360	180

Total Claims	Extra Claims	Fee ($)	Fee Paid ($)
_____ - = _____	x _____ =	_____	

HP = highest number of total claims paid for, if greater than 20.

Indep. Claims	Extra Claims	Fee ($)	Fee Paid ($)
_____ - = _____	x _____ =	_____	

HP = highest number of independent claims paid for, if greater than 3.

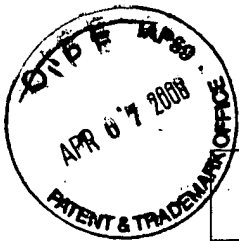| Multiple Dependent Claims	
Fee ($)	Fee Paid ($)
_____	_____

3. APPLICATION SIZE FEE

If the specification and drawings exceed 100 sheets of paper (excluding electronically filed sequence or computer listings under 37 CFR 1.52(e)), the application size fee due is $260 ($130 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).

Total Sheets	Extra Sheets	Number of each additional 50 or fraction thereof	Fee ($)	Fee Paid ($)
_____ - 100 =	_____ /50 =	_____ (round up to a whole number) x	_____ =	_____

4. OTHER FEE(S)

Non-English Specification, $130 fee (no small entity discount)

	Fees Paid ($)
Other (e.g., late filing surcharge): 1402 Filing a brief in support of an appeal	510.00

SUBMITTED BY			
Signature	~~signature~~ 40,290	Registration No. (Attorney/Agent) 24,104 / 40,290	Telephone (202) 955-3750
Name (Print/Type)	Ronald P. Kananen Christopher M. Tobin		Date April 7, 2008

TRANSMITTAL OF APPEAL BRIEF			Docket No. SON-2356

In re Application of: Akira Kimura

Application No. 10/082,186-Conf. #4346	Filing Date February 26, 2002	Examiner M. J. Pyzocha	Group Art Unit 2137

Invention: AUTHENTICATION SYSTEM AND METHOD, IDENTIFICATION INFORMATION INPUTTING METHOD AND APPARATUS ANDS PORTABLE TERMINAL

TO THE COMMISSIONER OF PATENTS:

Transmitted herewith is the Appeal Brief in this application, with respect to the Notice of Appeal filed: ___February 14, 2008___ .

The fee for filing this Appeal Brief is ___$ 510.00___ .

[x] Large Entity   [ ] Small Entity

[x] A petition for extension of time is also enclosed.

  The fee for the extension of time is _____ .

[ ] A check in the amount of _____ is enclosed.

[x] Charge the amount of the fee to Deposit Account No. ___18-0013___ .
    This sheet is submitted in duplicate.

[ ] Payment by credit card. Form PTO-2038 is attached.

[x] The Director is hereby authorized to charge any additional fees that may be required or credit any overpayment to Deposit Account No. ___18-0013___ .
    This sheet is submitted in duplicate.

Dated: ___April 7, 2008___

Ronald P. Kananen / Christopher M. Tobin
Attorney Reg. No. : 24,104 – 40,290
RADER, FISHMAN & GRAUER PLLC
1233 20th Street, N.W.
Suite 501
Washington, DC 20036
(202) 955-3750
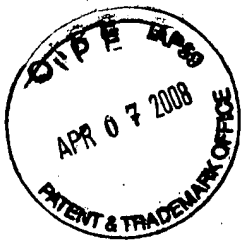
Docket No.: SON-2356
(PATENT)

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:

Akiru KIMURA

Application No.: 10/082,186   Confirmation No.: 4346

Filed: February 26, 2002   Art Unit: 2137

For: AUTHENTICATION SYSTEM AND METHOD   Examiner: M. J. Pyzocha
     INDENTIFICATION INFORMATION
     INPUTTING METHOD AND APPARATUS
     AND PORTABLE TERMINAL

APPEAL BRIEF

MS Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

  This is an Appeal Brief under 37 C.F.R. § 41.37 appealing the final decision of the Examiner dated December 14, 2007. This Brief is also in furtherance of the Notice of Appeal previously filed on February 14, 2008.

This brief contains items under the following headings as required by 37 C.F.R. § 41.37 and M.P.E.P. § 1206:

I.   Real Party In Interest
II   Related Appeals and Interferences
III.   Status of Claims
IV.   Status of Amendments
V.   Summary of Claimed Subject Matter
VI.   Grounds of Rejection to be Reviewed on Appeal
VII.   Argument
VIII.   Claims
IX.   Evidence
X.   Related Proceedings

Appendix A   Claims

Appendix B   Additional Evidence (none)

Appendix C   Related Proceedings (none)

I.   REAL PARTY IN INTEREST

The real party in interest for this appeal is Sony Corporation, of Tokyo, Japan. An assignment of all rights in the present application to Sony Corporation was executed by the inventors and recorded by the United States Patent and Trademark Office at Reel 013090, Frame 0367.

II.   RELATED APPEALS, INTERFERENCES, AND JUDICIAL PROCEEDINGS

There are no other appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in this appeal.

III.   STATUS OF CLAIMS

    A. Current Status of Claims

    A complete listing of the claims with corresponding status is provided as follows:

    Claim 1. (Rejected).

    Claim 2. (Rejected).

    Claim 3. (Rejected).

    Claim 4. (Rejected).

    Claim 5. (Rejected).

    Claim 6. (Rejected).

    Claim 7. (Rejected).

    Claim 8. (Rejected).

    Claim 9. (Rejected).

    Claim 10. (Rejected).

    Claim 11. (Rejected).

    Claim 12. (Rejected).

    Claim 13. (Rejected).

    Claim 14. (Rejected).

    Claim 15. (Rejected).

    Claim 16. (Rejected).

    Claim 17. (Rejected).

    Claim 18. (Rejected).

Claim 19. (Rejected).

Claim 20. (Rejected).

Claim 21. (Rejected).

Claim 22. (Rejected).

Claim 23. (Rejected).

Claim 24. (Rejected).

Claim 25. (Canceled).

Claim 26. (Canceled).

Claim 27. (Canceled).

Claim 28. (Canceled).

Claim 29. (Canceled).

Claim 30. (Canceled).

Claim 31. (Canceled).

Claim 32. (Canceled).

Claim 33. (Canceled).

Claim 34. (Canceled).

Claim 35. (Rejected).

Claim 36. (Rejected).

Claim 37. (Rejected).

Claim 38. (Rejected).

Claim 39. (Rejected).

Claim 40. (Rejected).

Claim 41. (Rejected).

Claim 42. (Rejected).

Claim 43. (Rejected).

Claim 44. (Rejected).

Claim 45. (Rejected).

Claim 46. (Rejected).

B.   Claims On Appeal

Appellant hereby appeals the final rejection of claims 1-24 and 35-46.

IV.   STATUS OF AMENDMENTS

An Appeal Brief was previously filed in this application, on January 17, 2007 with resubmission on April 17, 2007. Following this, prosecution was re-opened and a new Non-Final Rejection was mailed on August 2, 2007. An Amendment in response to the new Non-Final Action was submitted November 1, 2007, with corresponding Remarks traversing the rejections of record, and that Amendment was duly entered and considered by the Office. A Final Rejection of the claims of record was mailed on December 14, 2007, and Appellant filed a Notice of Appeal on February 14, 2008.

V.   SUMMARY OF CLAIMED SUBJECT MATTER

The following description is for illustrative purposes and is not intended to limit the scope of the invention.

By way of introduction, certain embodiments of Appellant's claimed invention provide techniques for protecting unauthorized access to private information in a situation where

a user accesses information using a portable card terminal (e.g, FIGs. 3-6, element 10) that communicates with an authentication system (e.g., FIGs. 2-3, element 20). For example, independent claim 1 recites authentication features involving the first identification information (e.g., the portable card terminal ID), correlated generation of an encryption key, and encryption of second identification information input to the portable card terminal using the encryption key. Specifically, the claim recites authentication wherein (1) the "first identification information" (further recited as the portable card ID) is sent from the portable card terminal to the authentication device (e.g., as illustrated in FIG.1, S2), (2) the authentication device generates the encryption key in response to receiving the first identification information (e.g., FIG. 1, S3), (3) the authentication device sends the so-generated encryption key back to the portable terminal device (e.g., FIG. 1, S4), and (4) the portable terminal device then uses the encryption key to encrypt second identification information input to the portable card terminal (e.g., the PIN entered by the user) and sends this encrypted second identification information to the authentication device (e.g., FIG. 1, S4), which then performs authentication (e.g., FIG. 1, S5).

Independent claim 1 recites: An authentication system (e.g., FIGs. 2-3, element 1, specification p. 28, line 11 through p. 36, line 4), said authentication system comprising:a portable card terminal (e.g., FIGs. 2-6, element 10, specification p. 28, line 11 through p. 36, line 4), including:

first identification information storage means (e.g., FIGs. 2-3, element 11, specification p. 29, line 12 through p. 30, line 4; p. 21) having a first identification information stored therein for discriminating said portable card terminal, said first identification information comprising a portable card terminal identifier that uniquely identifies the portable card terminal,

operating means (e.g., FIGs. 2-3, element 12, specification p. 35, line 8 through p. 36, line 4; p. 29-30; FIGs. 4-6; pp. 21, 35-49) for inputting a second identification information associated with said first identification information,

encryption means (e.g., FIGs. 2-3, element 14, specification p. 30, line 5 through p. 31, line 2; pp. 21-22, 34-36) for encrypting the second identification information input by said operating means based on encryption key information, and

first communication means (*e.g.*, FIGs. 2-3, element 13, specification p. 29, line 12 through p. 30, line 4; pp. 21-28) for communication with an authentication device, wherein said communication includes transmitting the first identification information to said authentication device and receiving said encryption key information from the authentication device in response to transmitting the first identification information;

said authentication device (*e.g.*, FIGs. 2-3, element 20, specification p. 28, line 11 through p. 29, line 11), provided independently of said portable card terminal for communication with said portable card terminal, the authentication device including:

second identification information storage means (*e.g.*, FIGs. 2-3, element 23, specification p. 32, line 3 through p. 34, line 15; pp. 21-26) for storage of the first identification information and the second identification information therein,

encryption key information generating means (*e.g.*, FIGs. 2-3, element 22, specification p. 32, line 3 through p. 33 line 19; p. 22) for generating said encryption key information, wherein said encryption key information comprises a random number, and wherein said encryption key information is generated in response to receiving the first identification information from said portable terminal,

second communication means (*e.g.*, FIGs. 2-3, element 21; specification p. 32, line 3 through p. 36, line 4; pp. 21-28) for communication with said portable card terminal, and

comparator authentication means (*e.g.*, FIGs. 2-3, elements 25, 28, specification p. 32, line 3 through p. 36, line 4) for comparing and authenticating the second identification information encrypted by said encryption means based on said encryption key information;

wherein said portable card terminal encrypts the second identification information input from said operating means, based on said encryption key information received from said authentication device, the so-encrypted second identification information is transmitted through said first communication means to said authentication device (*e.g.*, specification pp. 21-28, 30-32, 34-36); and

7

wherein, in said authentication device, the encrypted second identification information received through said second communication means and the second identification information stored by said second identification information storage means are compared to each other based on said encryption key information to perform the authentication (*e.g.*, specification pp. 21-28, 32-36).

Dependent claim 6 recites: The authentication system according to claim 4, wherein said portable card terminal includes a transient storage means in which the second identification information is stored transiently (*e.g.*, FIG. 1, specification p. 22, lines 3-21; pp. 23-24, 30).

Dependent claim 7 recites: The authentication system according to claim 6, wherein said transient storage means stores the second identification information input by said operating means until authentication of said portable card terminal by said authentication device (*e.g.*, FIG. 1, specification p. 22, lines 3-21; pp. 23-24, 30-31).

Dependent claim 8 recites: The authentication system according to claim 6, wherein said second identification information stored in said transient storage means is erased every preset time interval (*e.g.*, FIG. 1, specification p. 22, lines 3-21; pp. 23-24, 30-31).

Dependent claim 10 recites: The authentication system according to claim 4, wherein said operating means in said portable card terminal includes a plurality of input locations respectively used for indicating letters or numerical figures for inputting said second identification information, and wherein the input locations corresponding to individual ones of the letters or numerical figures are variable, such that individual ones of the letters or numerical figures are resident at one of the plurality of input locations when said second identification information is input a first time, and are resident at another of the plurality of input locations when said second identification information is input a second time (*e.g.*, FIGs. 4-6, specification pp. 36-39).

Independent claim 13 recites: An authentication method in which a portable card terminal is authenticated by an authentication device provided independently of said portable

8

card terminal (*e.g.*, FIG. 1, specification p. 20, line 21 through p. 28, line 10; FIGs. 2-3, element

1, specification p. 28, line 11 through p. 36, line 4), said method comprising

an operating step of inputting a second identification information associated with a first

identification information that discriminates said portable card terminal and that is stored in a

first identification information storage means of said portable card terminal, said first

identification information comprising a portable card terminal identifier that uniquely identifies

the portable card terminal (*e.g.*, FIG. 1, S1-S2, pp. 29-30; FIGs. 2-3, element 11, specification p.

29, line 12 through p. 30, line 4; p. 21; FIGs. 2-3, element 12, specification p. 35, line 8 through

p. 36, line 4; p. 29-30; FIGs. 4-6; pp. 21, 35-49),

an encryption key information generating step of generating an encryption key

information by transmitting the first identification information from the portable card terminal to

the authentication device, and receiving said encryption key information from the authentication

device in response to transmitting the first identification information, wherein said encryption

key information is generated by the authentication device in response to receiving the first

identification information from the portable card terminal (*e.g.*, FIG. 1, S2-S4, specification pp.

22-28; FIGs. 2-3, element 14, specification p. 30, line 5 through p. 31, line 2; pp. 21-22, 34-36;

FIGs. 2-3, element 13, specification p. 29, line 12 through p. 30, line 4; pp. 21-28FIGs. 2-3,

element 22, specification p. 32, line 3 through p. 33 line 19; p. 22),

an encrypting step of encrypting the second identification information input at said

operating step, based on the encryption key information generated in said encryption key

information generating step (*e.g.*, FIG. 1, S4, FIGs. 2-3, element 14, specification p. 30, line 5

through p. 31, line 2; pp. 21-22, 34-36), and

a comparison authentication step of comparing the second identification information

encrypted in said encrypting step to the second identification information as stored in a second

identification information storage means to perform the authentication (*e.g.*, FIG. 1, S5, FIGs. 2-

3, elements 25, 28, specification p. 32, line 3 through p. 36, line 4; pp. 21-28, 32-36).

Independent claim 35 recites: a portable card terminal authenticated by an authentication device (e.g., FIGs. 2-6, element 10, specification p. 28, line 11 through p. 36, line 4), comprising,

first identification information storage means (e.g., FIGs. 2-3, element 11, specification p. 29, line 12 through p. 30, line 4; p. 21) for storing a first identification information for discriminating said portable card terminal, said first identification information comprising a portable card terminal identifier that uniquely identifies the portable card terminal,

operating means (e.g., FIGs. 2-3, element 12, specification p. 35, line 8 through p. 36, line 4; p. 29-30; FIGs. 4-6; pp. 21, 35-49) for inputting a second identification information associated with said first identification information,

communication means (e.g., FIGs. 2-3, element 13, specification p. 29, line 12 through p. 30, line 4; pp. 21-28) for communication with said authentication device wherein said communication including transmitting the first identification information from the portable card terminal to the authentication device, and receiving encryption key information from the authentication device in response to transmitting the first identification information, and

encrypting means (e.g., FIGs. 2-3, element 14, specification p. 30, line 5 through p. 31, line 2; pp. 21-22, 34-36) for encrypting the second identification information input by said operating means based on said encryption key information received from said authentication device, wherein said encryption key information is generated by the authentication device in response to receiving the first identification information from the portable card terminal (e.g., FIGs. 2-3, element 14, specification p. 30, line 5 through p. 31, line 2; pp. 21-22, 34-36; 21-28, 32-36).

Independent claim 46 recites: An authentication system (e.g., FIGs. 2-3, element 1, specification p. 28, line 11 through p. 36, line 4) made up by a portable card terminal and an authentication device provided independently of said portable card terminal for communication with said portable card terminal, said authentication system comprising:

said portable card terminal (*e.g.*, FIGs. 2-6, element 10, specification p. 28, line 11 through p. 36, line 4), including

first identification information storage means (*e.g.*, FIGs. 2-3, element 11, specification p. 29, line 12 through p. 30, line 4; p. 21) having a first identification information stored therein for discriminating said portable card terminal, said first identification information comprising a portable card terminal identifier that uniquely identifies the portable card terminal,

operating means (*e.g.*, FIGs. 2-3, element 12, specification p. 35, line 8 through p. 36, line 4; p. 29-30; FIGs. 4-6; pp. 21, 35-49) including display means for irregularly displaying letters included in a group of letters and selection means for selecting the letters making up a second identification information from among the letters irregularly displayed on said display means, said operating means inputting the second identification information associated with said first identification information,

encryption means (*e.g.*, FIGs. 2-3, element 14, specification p. 30, line 5 through p. 31, line 2; pp. 21-22, 34-36) for encrypting the second identification information input by said operating means based on an encryption key information, and

first communication means (*e.g.*, FIGs. 2-3, element 13, specification p. 29, line 12 through p. 30, line 4; pp. 21-28) for communication with said authentication device, wherein said communication includes transmitting the first identification information to said authentication device and receiving said encryption key information from the authentication device in response to transmitting the first identification information;

said authentication device (*e.g.*, FIGs. 2-3, element 20, specification p. 28, line 11 through p. 29, line 11), including

second identification information storage means (*e.g.*, FIGs. 2-3, element 23, specification p. 32, line 3 through p. 34, line 15; pp. 21-26) having the first identification information and the second identification information stored therein,

encryption key information generating means (*e.g.*, FIGs. 2-3, element 22, specification p. 32, line 3 through p. 33 line 19; p. 22) for generating said encryption key information, wherein said encryption key information is generated in response to receiving the first identification information from said portable terminal,

second communication means (*e.g.*, FIGs. 2-3, element 21; specification p. 32, line 3 through p. 36, line 4; pp. 21-28) for communication with said portable card terminal, and

comparator authentication means (*e.g.*, FIGs. 2-3, elements 25, 28, specification p. 32, line 3 through p. 36, line 4) for comparing the second identification information encrypted by said encryption means to the second identification information stored in the second identification information storage means; wherein

said portable card terminal encrypts the second identification information input from said operating means, based on said encryption key information received from said authentication device through said first communication means, and the so-encrypted second identification information is transmitted through said first communication means to said authentication device (*e.g.*, specification pp. 21-28, 30-32, 34-36); and

wherein, in said authentication device, the encrypted second identification information received through said second communication means and the second identification information stored by said second identification information storage means are compared to each other based on said encryption key information to perform the authentication (*e.g.*, specification pp. 21-28, 32-36).

VI.   GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

The issues presented for consideration in this appeal, with separate arguments as noted in the following sections, are as follows:

Whether the Examiner erred in rejecting claims 1-9, 13-21 and 35-42 under 35 U.S.C. § 103(a) as being unpatentable over U.S. Pat. No. 6,286,099 to Kramer ("Kramer") in view of U.S. Pat. No. 5,880,769 to Nemirofsky ("Nemirofsky").

Whether the Examiner erred in rejecting claims 10-12, 22-24 and 43-46 under 35 U.S.C. § 103(a) as being unpatentable over Kramer in view of Nemirofsky, and further in view of U.S. Pat. No. 5,919,090 to Bell et al. ("Bell").

These issues are discussed in the following section.

VII.   ARGUMENT

In the Final Office Action of August 23, 2006, the Examiner erred in rejecting claims 1-9, 13-21 and 35-42 under 35 U.S.C. § 103(a) as being unpatentable over U.S. Pat. No. 6,286,099 to Kramer ("Kramer") in view of U.S. Pat. No. 5,880,769 to Nemirofsky ("Nemirofsky"), and erred in rejecting claims 10-12, 22-24 and 43-46 under 35 U.S.C. § 103(a) as being unpatentable over Kramer in view of Nemirofsky, and further in view of U.S. Pat. No. 5,919,090 to Bell et al. ("Bell"). Consistent with the grouping of claims in the following section, these rejections are variously deficient as noted in the separate arguments.

VII.A.   Grouping of claims: Claims 1-24 and 35-46 are currently pending in the application. Claims 1-5 and 35-38 stand or fall together. Claims 13-17 stand or fall together. Claims 6, 9, 18, 21, 39 and 42 stand or fall together. Claims 7, 19 and 40 stand or fall together. Claims 8, 20 and 41 stand or fall together. Claims 10-12, 22-24 and 43-46 stand or fall together.

VII.B   The Examiner erred in rejecting claims 1-5 and 35-38 under 35 U.S.C. § 103(a) as being unpatentable over U.S. Pat. No. 6,286,099 to Kramer in view of U.S. Pat. No. 5,880,769 to Nemirofsky.

Independent claim 1 recites: *[a]n authentication system, said authentication system comprising:*

a portable card terminal, including:

first identification information storage means having a first identification information stored therein for discriminating said portable card terminal, said first identification information comprising a portable card terminal identifier that uniquely identifies the portable card terminal,

operating means for inputting a second identification information associated with said first identification information,

encryption means for encrypting the second identification information input by said operating means based on encryption key information, and

first communication means for communication with an authentication device, wherein said communication includes transmitting the first identification information to said authentication device and receiving said encryption key information from the authentication device in response to transmitting the first identification information;

said authentication device, provided independently of said portable card terminal for communication with said portable card terminal, the authentication device including:

second identification information storage means for storage of the first identification information and the second identification information therein,

encryption key information generating means for generating said encryption key information, wherein said encryption key information comprises a random number, and wherein said encryption key information is generated in response to receiving the first identification information from said portable terminal,

second communication means for communication with said portable card terminal, and

14

comparator authentication means for comparing and authenticating the second identification information encrypted by said encryption means based on said encryption key information;

wherein said portable card terminal encrypts the second identification information input from said operating means, based on said encryption key information received from said authentication device, the so-encrypted second identification information is transmitted through said first communication means to said authentication device; and

wherein, in said authentication device, the encrypted second identification information received through said second communication means and the second identification information stored by said second identification information storage means are compared to each other based on said encryption key information to perform the authentication.

Appellant's claimed invention provides a technique for protecting unauthorized access to private information in a situation where the user accesses information using a portable card terminal that communicates with an authentication system. Independent claim 1 recites authentication features involving the first identification information (*e.g.*, the portable card terminal ID), correlated generation of an encryption key, and encryption of second identification information input to the portable card terminal using the encryption key. Specifically, the claim recites authentication wherein (1) the "first identification information" (further recited as the portable card ID) is sent from the portable card terminal to the authentication device, (2) the authentication device generates the encryption key in response to receiving the first identification information, (3) the authentication device sends the so-generated encryption key back to the portable terminal device, and (4) the portable terminal device then uses the encryption key to encrypt second identification information input to the portable card terminal (*e.g.*, the PIN entered by the user) and sends this encrypted second identification information to the authentication device, which then performs authentication.

Kramer and Nemirofsky to do not disclose or suggest the features recited in claim 1, whether alone or in any combination.

Kramer merely appears to disclose that a session key may be generated and used to accommodate the encryption of communications between two devices. As noted by the

Examiner, Kramer does not disclose a portable card terminal with operating means for inputting second identification information associated with the first identification information.

The Examiner refers to FIGs. 4 and 6 and some related description in Kramer as purportedly disclosing all but the portable card terminal with operating means for inputting the second identification information. However, Appellant submits that more than just these claimed features are absent from Kramer, as Kramer does not appear to send the first identification information from the portable terminal to the authentication device, then have the authentication device generate an encryption key and send it to the portable terminal, and finally have the portable terminal device use the encryption key to encrypt the second identification information.

FIG. 5 appears to disclose a flow of messages between a "POI Device" 5000 and a Financial Institution (FI) 5100, wherein the POI device sends keys, and optionally a "Device Properties Descriptor" (DPD), to the FI, which then returns a public key back to the POI device. The POI device uses the public key of the FI to encrypt communications so that only the FI can decrypt them. In this scheme, the public key is the public key of the FI, and not a particular key that is generated and associated to the POI device based upon its first identification information. FIG. 6, and column 9, lines 35-48 appear to disclose a similar sequence, but with a session key sent in the permission message. There is clearly no description of the sequence of sending the first identification information from the portable terminal to the authentication device, then having the authentication device generate an encryption key and send it to the portable terminal, and finally having the portable terminal device use the encryption key to encrypt the second identification information.

The Final Office Action dated December 14, 2007 alleges that Kramer discloses sending first identification information, an authentication device generating a key that is sent back to the portable device, and encrypting the second identification information with a key. (Action, at p. 9). With regard to the first item, it is alleged that in Kramer the POI sends its public keys and the Device Properties Descriptor in a request to the FI (citing column 8, lines 55-59 of Kramer).

16

The Action states that the keys and the DPD are the first identification information. (Action, at p. 9). However, this position ignores what is actually recited for the first identification information. That is, as clearly recited in claim 1, "*said first identification information compris[es] a portable card terminal identifier that uniquely identifies the portable card terminal.*"

Neither the keys nor the DPD uniquely identify any kind of device. They are not unique device identifiers. The public key is not a unique device identifier. It is, rather, a number that can be commonly used by any number of devices. Indeed, the embodiments in Kramer contemplate such sharing. For example, as described in Kramer, the POI device includes the public key of a consortium of banks (the consortium key) that wish to share the use of a pool of POI devices. (Kramer, at column 6, lines 46-63). In no instance does Kramer in any way express or imply that the public key is in any way a unique device identifier.

The DPD is also clearly not a unique device identifier. The DPD merely describes the general properties of the device. For example, Kramer states that:

"Device properties database 4400 is used to look up information about a POI device (*e.g.*, POI device 4000) that is not conveyed by the POI device itself. Some examples of the types of information that can be stored include the following:

> The device manufacturer as a function of the device public key certificate of the POI device. This information is advantageous if, for example, the POI device is so memory-restricted that the key cannot be signed.
>
> The POI device properties as a function of the device public key certificate of the POI device. This is advantageous if, for example, the POI device does not have enough memory to store a signed description of its properties.
>
> Allowed transactions as a function of the POI device properties. In practice, this information is most likely to be kept by the FI and will be specific to the policies set by the FI. For example, some smart-card reader devices reside in the floppy drive of a computer, but use the keyboard to enter a PIN to unlock the device. A FI may decide not to allow transactions from such a device, because the keyboard driver, floppy device driver, and the application program are all subject to attack, as discussed above. However, another FI may allow transactions from such a device. " (Kramer, at column 8, lines 25-45).

The above passage clearly illustrates that the DPD pertains to the general characteristics of possible devices, rather than uniquely identifying a device. The DPD is thus another example of information that does not qualify as an example of the particular first information claimed by Appellant.

Nemirofsky discloses a smart card that stores account information for remote financial services. A connection with a financial institution is initiated through the smart card, and data is exchanged to carry out a fully automated transaction. A user may also be required to enter a PIN code that is associated with the smart card, for enhanced security.

Although, as noted in the Action, Nemirofsky is merely relied upon for disclosing a smartcard, it is reiterated that Nemirofsky makes no mention of encrypting the PIN code. In that sense, Nemirofsky appears to disclose a typical banking card type exchange, wherein the user enters the PIN code and that information allows the user to continue access to financial or other information. There is no mention of encrypting the PIN code even generally, let alone according to the specific exchange of information claimed by Appellant. At best, Nemirofsky uses a PIN that is sent to the authentication device. There is no mention in the reference of (1) sending the "first identification information" (the portable card ID) from the portable card terminal to the authentication device, (2) having the authentication device generate the encryption key in response to receiving the first identification information, (3) having the authentication send the so-generated encryption key back to the portable terminal device, (4) then having the portable terminal device use the encryption key to encrypt second identification information that is input to the portable card terminal (*e.g.*, the PIN entered by the user) and send the encrypted second identification information to the authentication device, which finally performs authentication. These deficiencies of Nemirofsky are noted because, as noted above, Kramer is variously deficient in this regard as well.

Therefore, Appellant submits that, even assuming for the sake of argument that motivation to combine the references is present, a *prima facie* case of obviousness remains absent. This is because even a combination of the references would still fail to yield various features of the claimed invention for the reasons noted above.

18

Accordingly, Appellant respectfully requests reversal of the Examiner's rejection of claims 1-5 and 35-38 under 35 U.S.C. § 103(a) as being unpatentable over Kramer in view of Nemirofsky.

VII.C   The Examiner erred in rejecting claims 13-17 under 35 U.S.C. § 103(a) as being unpatentable over Kramer in view of Nemirofsky.

Claim 13 recites: *An authentication method in which a portable card terminal is authenticated by an authentication device provided independently of said portable card terminal, said method comprising*

an operating step of inputting a second identification information associated with a first identification information that discriminates said portable card terminal and that is stored in a first identification information storage means of said portable card terminal, said first identification information comprising a portable card terminal identifier that uniquely identifies the portable card terminal,

an encryption key information generating step of generating an encryption key information by transmitting the first identification information from the portable card terminal to the authentication device, and receiving said encryption key information from the authentication device in response to transmitting the first identification information, wherein said encryption key information is generated by the authentication device in response to receiving the first identification information from the portable card terminal,

an encrypting step of encrypting the second identification information input at said operating step, based on the encryption key information generated in said encryption key information generating step, and

a comparison authentication step of comparing the second identification information encrypted in said encrypting step to the second identification information as stored in a second identification information storage means to perform the authentication.

Kramer and Nemirofsky to do not disclose or suggest the features recited in claim 13, whether alone or in any combination.

As noted previously, Kramer discloses generating a session key that is used to accommodate the encryption of communications between two devices. Kramer does not disclose a portable card terminal with operating means for inputting second identification information associated with the first identification information, and variously fails to disclose implementation of the first identification information or the corresponding claimed processing sequence.

FIG. 5 of Kramer, which is relied upon as purportedly disclosing such features, appears to disclose a flow of messages between a "POI Device" 5000 and a Financial Institution (FI) 5100, wherein the POI device sends keys, and optionally a "Device Properties Descriptor" (DPD), to the FI, which then returns a public key back to the POI device. The POI device uses the public key of the FI to encrypt communications so that only the FI can decrypt them. In this scheme, the public key is the public key of the FI, and not a particular key that is generated and associated to the POI device based upon its first identification information. FIG. 6, and column 9, lines 35-48 appear to disclose a similar sequence, but with a session key sent in the permission message. There is clearly no description of the sequence of sending the first identification information from the portable terminal to the authentication device, then having the authentication device generate an encryption key and send it to the portable terminal, and finally having the portable terminal device use the encryption key to encrypt the second identification information.

The Final Office Action dated December 14, 2007 posits that Kramer discloses sending first identification information, an authentication device generating a key that is sent back to the portable device, and encrypting the second identification information with a key. (Action, at p. 9). With regard to the first item, it is alleged that in Kramer the POI sends its public keys and the Device Properties Descriptor in a request to the FI (citing column 8, lines 55-59 of Kramer). However, this position ignores what is actually recited for the first identification information. That is, as clearly recited in claim 1, "*said first identification information compris[es] a portable card terminal identifier that uniquely identifies the portable card terminal.*"

As noted previously the keys and the DPD are not unique identifiers for a device. The public key is not a unique device identifier, but is instead a number that can be commonly

20

required by any number of devices, as noted in the previous section. In no instance does Kramer in any way express or imply that the public key is in any way a unique device identifier. The DPD is also clearly not a unique device identifier. The DPD merely describes the general properties or characteristics of possible devices, and also fails to disclose unique device identification as claimed by Appellant.

Nemirofsky discloses a smart card that stores account information for remote financial services. A connection with a financial institution is initiated through the smart card, and data is exchanged to carry out a fully automated transaction. A user may also be required to enter a PIN code that is associated with the smart card, for enhanced security.

As also noted previously, Nemirofsky is relied upon for disclosing a smartcard, and does not disclose or suggest encrypting the PIN code. In that sense, Nemirofsky appears to disclose a typical banking card type exchange, wherein the user enters the PIN code and that information allows the user to continue access to financial or other information. There is no mention of encrypting the PIN code even generally, let alone according to the specific exchange of information claimed by Appellant. At best, Nemirofsky uses a PIN that is sent to the authentication device. There is no mention in the reference of (1) sending the "first identification information" (the portable card ID) from the portable card terminal to the authentication device, (2) having the authentication device generate the encryption key in response to receiving the first identification information, (3) having the authentication send the so-generated encryption key back to the portable terminal device, (4) then having the portable terminal device use the encryption key to encrypt second identification information that is input to the portable card terminal (*e.g.*, the PIN entered by the user) and send the encrypted second identification information to the authentication device, which finally performs authentication.

Appellant submits that, since even the combination of references would still fail to yield the features of claim 13, a *prima facie* case has not been presented.

Accordingly, Appellant respectfully requests reversal of the Examiner's rejection of claims 13-17 under 35 U.S.C. § 103(a) as being unpatentable over Kramer in view of Nemirofsky.

VII.D   The Examiner erred in rejecting claims 6, 9, 18, 21, 39 and 42 under 35 U.S.C. § 103(a) as being unpatentable over Kramer in view of Nemirofsky.

Claim 6 recites: *wherein said portable card terminal includes a transient storage means in which the second identification information is stored transiently.*

There is no mention of any kind in either reference of transiently storing the second identification information. At best, both references make passing references to a PIN at best, but there is no discussion of any kind of transiently storing the PIN (or the other related features, as noted above, which need not be repeated in this section).

Accordingly, Appellant respectfully requests reversal of the Examiner's rejection of claims 6, 9, 18, 21, 39 and 42 under 35 under 35 U.S.C. § 103(a) as being unpatentable over Kramer in view of Nemirofsky.

VII.E   The Examiner erred in rejecting claims 7, 19 and 40 under 35 U.S.C. § 103(a) as being unpatentable over Kramer in view of Nemirofsky.

Claim 7 recites: *The authentication system according to claim 6, wherein said transient storage means stores the second identification information input by said operating means until authentication of said portable card terminal by said authentication device.*

There is no mention of any treatment of any kind regarding the PIN in either Kramer or Nemirofsky. As the references are silent as to whether they even generally consider transiently storing the information, there is clearly no disclosure or suggestion of making storage contingent upon whether the authentication process has been successfully completed, as claimed by Appellant.

Accordingly, Appellant respectfully requests reversal of the Examiner's rejection of claims 7, 19 and 40 under 35 under 35 U.S.C. § 103(a) as being unpatentable over Kramer in view of Nemirofsky.

VII.F   The Examiner erred in rejecting claims 8, 20 and 41 under 35 U.S.C. § 103(a) as being unpatentable over Kramer in view of Nemirofsky.

Claim 8 recites: *The authentication system according to claim 6, wherein said second identification information stored in said transient storage means is erased every preset time interval.*

Again, Kramer and Nemirofsky are silent as to any transient retention of the second information such as a PIN. There is clearly also no disclosure or suggestion of erasing such information every preset time interval as claimed by Appellant. As to the contention that Official Notice was taken regarding this feature, it is reiterated that objection was made to any and all taking of such Notice, and it was also specified that any prior taking of Official Notice regarding a claim is moot and inapplicable to a subsequent claim that was amended (and that thus presented issues in a different context as compared to the alleged prior instance).

Accordingly, the features are clearly not disclosed, suggested, or admitted as having been presented in the references of record, and thus Appellant respectfully requests reversal of the Examiner's rejection of claims 8, 20 and 41 under 35 under 35 U.S.C. § 103(a) as being unpatentable over Kramer in view of Nemirofsky.

VII.G   The Examiner erred in rejecting claims 10-12, 22-24 and 43-46 under 35 U.S.C. § 103(a) as being unpatentable over Kramer in view of Nemirofsky, and further in view of Bell.

Claim 10 recites: *The authentication system according to claim 4, wherein said operating means in said portable card terminal includes a plurality of input locations respectively used for indicating letters or numerical figures for inputting said second identification information, and wherein the input locations corresponding to individual ones of the letters or numerical figures are variable, such that individual ones of the letters or numerical figures are resident at one of the plurality of input locations when said second identification information is input a first time, and are resident at another of the plurality of input locations when said second identification information is input a second time.*

Kramer and Nemirofsky are variously deficient in that they fail to disclose the features recited in claim 1 and other claims as noted above. Claim 10 indirectly depends from claim 1 and thus incorporates those features. Bell does not remedy the deficiencies of Kramer and Nemirofsky. Bell discloses a gaming machine system which is clearly a distinct field from

the authentication system claimed by Appellant. Moreover, although column 7, lines 1-35 of Bell bear some superficial similarity to the claimed features, in Bell the description is to altering the position of numbers as different customers use an ATM. This is clearly distinct from having such a function in one individual user's portable card terminal, wherein the position of input locations changes when the *same* customer enters the PIN a second time using the device.

Accordingly, these claimed features are clearly not disclosed or suggested by the relied upon references, and thus Appellant respectfully requests reversal of the Examiner's rejection of claims 10-12, 22-24 and 43-46 under 35 under 35 U.S.C. § 103(a) as being unpatentable over Kramer in view of Nemirofsky.

VIII.   CLAIMS

A copy of the claims involved in the present appeal is attached hereto as Appendix A.

IX.   EVIDENCE

No evidence pursuant to §§ 1.130, 1.131, or 1.132, or additional evidence entered by or relied upon by the Examiner is being submitted.

X.   RELATED PROCEEDINGS

No related proceedings are referenced in section II above, or copies of decisions in related proceedings are not provided.

Conclusion

     The claims are considered allowable for the same reasons discussed above, as well as for the additional features they recite.

     Reversal of the Examiner's decision is respectfully requested.

Dated: April 7, 2008   Respectfully submitted,

By_____
Ronald P. Kananen
   Registration No.: 24,104
Christopher M. Tobin
   Registration No.: 40,290
RADER, FISHMAN & GRAUER PLLC
Correspondence Customer Number: 23353
Attorney for Appellant

APPENDIX A - CLAIMS

1. (Previously Presented) An authentication system, said authentication system comprising:

a portable card terminal, including:

first identification information storage means having a first identification information stored therein for discriminating said portable card terminal, said first identification information comprising a portable card terminal identifier that uniquely identifies the portable card terminal,

operating means for inputting a second identification information associated with said first identification information,

encryption means for encrypting the second identification information input by said operating means based on encryption key information, and

first communication means for communication with an authentication device, wherein said communication includes transmitting the first identification information to said authentication device and receiving said encryption key information from the authentication device in response to transmitting the first identification information;

said authentication device, provided independently of said portable card terminal for communication with said portable card terminal, the authentication device including:

second identification information storage means for storage of the first identification information and the second identification information therein,

encryption key information generating means for generating said encryption key information, wherein said encryption key information comprises a random number, and wherein said encryption key information is generated in response to receiving the first identification information from said portable terminal,

second communication means for communication with said portable card terminal, and

comparator authentication means for comparing and authenticating the second identification information encrypted by said encryption means based on said encryption key information;

wherein said portable card terminal encrypts the second identification information input from said operating means, based on said encryption key information received from said authentication device, the so-encrypted second identification information is transmitted through said first communication means to said authentication device; and

wherein, in said authentication device, the encrypted second identification information received through said second communication means and the second identification information stored by said second identification information storage means are compared to each other based on said encryption key information to perform the authentication.

2. (Previously Presented) The authentication system according to claim 1 wherein said authentication device includes:

decoding means for decoding the second identification information encrypted by said encrypting means based on said encryption key information,

said authentication device decoding the received encrypted second identification information based on said encryption key information, said authentication device comparing the decoded second identification information to the second identification information stored in said second identification information storage means, by way of performing the authentication.

3. (Previously Presented) The authentication system according to claim 2, wherein said second identification information is a password of a service user made up of a preset letter string or a preset string of numerical figures,

27

4. (Previously Presented)   The authentication system according to claim 3 for authenticating the service user to whom preset services are offered from a service provider in a credit sale system, an inter-account instant payment system and in E-commerce carried out over a preset network, wherein

said portable card terminal is a card-shaped portable terminal issued by said service provider to said service user,

said authentication device being contained in a host computer in which said service provider authenticates usage by said service user, and

said service user being authenticated by said authentication device authenticating said portable card terminal and that said service user is a true owner of the portable card terminal.

5. (Previously Presented) The authentication system according to claim 4, wherein said first and second communication means are wireless communication means.

6. (Previously Presented) The authentication system according to claim 4, wherein said portable card terminal includes a transient storage means in which the second identification information is stored transiently.

7. (Previously Presented) The authentication system according to claim 6, wherein said transient storage means stores the second identification information input by said operating means until authentication of said portable card terminal by said authentication device.

8. (Previously Presented) The authentication system according to claim 6, wherein said

second identification information stored in said transient storage means is erased every preset

time interval.

9. (Previously Presented) The authentication system according to claim 6, wherein said

operating means in said portable card terminal includes means for erasing the second

identification information stored in said transient storage means.

10. (Previously Presented) The authentication system according to claim 4, wherein said

operating means in said portable card terminal includes a plurality of input locations respectively

used for indicating letters or numerical figures for inputting said second identification

information, and wherein the input locations corresponding to individual ones of the letters or

numerical figures are variable, such that individual ones of the letters or numerical figures are

resident at one of the plurality of input locations when said second identification information is

input a first time, and are resident at another of the plurality of input locations when said second

identification information is input a second time.

11. (Previously Presented) The authentication system according to claim 10, wherein the

plurality of input locations are varied prior to the inputting of said second identification

information.

12. (Previously Presented) The authentication system according to claim 4, wherein said

operating means in said portable card terminal includes a display unit for displaying letters and a

selection unit for selecting the letters displayed on said display unit, and wherein the second

identification information input by said operating means is made up by a string of letters selected

by said selection unit from among plural letters sequentially displayed on said display unit.

13. (Previously Presented) An authentication method in which a portable card terminal is

authenticated by an authentication device provided independently of said portable card terminal,

said method comprising

an operating step of inputting a second identification information associated with a first

identification information that discriminates said portable card terminal and that is stored in a

first identification information storage means of said portable card terminal, said first

identification information comprising a portable card terminal identifier that uniquely identifies

the portable card terminal,

an encryption key information generating step of generating an encryption key

information by transmitting the first identification information from the portable card terminal to

the authentication device, and receiving said encryption key information from the authentication

device in response to transmitting the first identification information, wherein said encryption

key information is generated by the authentication device in response to receiving the first

identification information from the portable card terminal,

an encrypting step of encrypting the second identification information input at said

operating step, based on the encryption key information generated in said encryption key

information generating step, and

a comparison authentication step of comparing the second identification information

encrypted in said encrypting step to the second identification information as stored in a second

identification information storage means to perform the authentication.

14. (Previously Presented) The authentication method according to claim 13 further comprising

a decoding step of decoding the second identification information, encrypted in said encrypting step, based on said encryption key information,

the encrypted second identification information being decoded in said decoding step based on said encryption key information, and the decoded second identification information being compared to the second identification information stored in said second identification information storage means by way of performing the authentication.

15. (Previously Presented) The authentication method according to claim 14, wherein the encryption key information comprises a random number.

16. (Previously Presented) The authentication method according to claim 15 for authenticating a service user to whom preset services are offered from a service provider in a credit sale system, an inter-account instant payment system and in E-commerce carried out over a preset network, wherein

said portable card terminal is a card-shaped portable terminal issued by said service provider to said service user,

said authentication device being an authentication device contained in a host computer in which said service provider authenticates usage by said service user, and

said service user being authenticated by said authentication device authenticating said portable card terminal and that said service user is a true owner of the portable card terminal.

17. (Previously Presented) The authentication method according to claim 16, wherein said portable card terminal and the authentication device are interconnected by wireless communication means.

18. (Previously Presented) The authentication method according to claim 16, wherein said portable card terminal includes a transient storage step of transiently storing the second identification information.

19. (Previously Presented) The authentication method according to claim 18, wherein said transient storage step stores the second identification information input in said operating step until authentication of said portable card terminal by said authentication device.

20. (Previously presented) The authentication method according to claim 18, wherein said second identification information stored in said transient storage step is erased every preset time interval.

21. (Previously presented) The authentication method according to claim 18, wherein said operating step includes a step of erasing the second identification information stored in said transient storage step.

22. (Previously Presented) The authentication method according to claim 16, wherein inputting said second identification information comprises using a plurality of input locations respectively indicating letters or numerical figures for inputting said second identification information, and wherein the input locations corresponding to individual ones of the letters or

numerical figures are variable, such that individual ones of the letters or numerical figures are

resident at one of the plurality of input locations when said second identification information is

input a first time, and are resident at another of the plurality of input locations when said second

identification information is input a second time.

23. (Previously Presented) The authentication method according to claim 22, wherein the

plurality of input locations are varied prior to inputting of said second identification information.

24. (Previously Presented) The authentication method according to claim 16, wherein

said operating step includes a display step of displaying letters and a selection step of selecting

the letters displayed in said display step, and wherein the second identification information input

by said operating step is made up by a string of letters selected in said selection step from among

plural letters sequentially displayed in said display step.

25. (Canceled)

26. (Canceled)

27. (Canceled)

28. (Canceled)

29. (Canceled)

30. (Canceled)

31. (Canceled)

32. (Canceled)

33. (Canceled).

34. (Canceled)

35. (Previously Presented) A portable card terminal authenticated by an authentication device, comprising,

first identification information storage means for storing a first identification information for discriminating said portable card terminal, said first identification information comprising a portable card terminal identifier that uniquely identifies the portable card terminal,

operating means for inputting a second identification information associated with said first identification information,

communication means for communication with said authentication device wherein said communication including transmitting the first identification information from the portable card terminal to the authentication device, and receiving encryption key information from the authentication device in response to transmitting the first identification information, and

encrypting means for encrypting the second identification information input by said operating means based on said encryption key information received from said authentication

device, wherein said encryption key information is generated by the authentication device in

response to receiving the first identification information from the portable card terminal.

36. (Previously Presented) The portable card terminal according to claim 35, wherein

said encryption key information comprises a random number.

37. (Previously Presented) The portable card terminal according to claim 35, wherein the

portable card terminal is issued to a service user by a service provider to offer preset services for

said service user in a credit sale system, an inter-account instant payment system and E-

commerce carried out over a preset network and is in the form of a card.

38. (Previously Presented) The portable card terminal according to claim 37, wherein

said communication means are wireless communication means.

39. (Previously Presented) The portable card terminal according to claim 37, wherein

said portable card terminal includes transient storage means in which the second identification

information is stored transiently.

40. (Previously Presented) The portable card terminal according to claim 39, wherein

said transient storage means stores the second identification information input by said operating

means until authentication of said portable card terminal by said authentication device.

41. (Previously Presented) The portable card terminal according to claim 39, wherein said second identification information stored in said transient storage means is erased every preset time interval.

42. (Previously Presented) The portable card terminal according to claim 39, wherein said operating means in said portable card terminal includes means for erasing the second identification information stored in said transient storage means.

43. (Previously Presented) The portable card terminal according to claim 37, wherein said operating means includes a plurality of input locations respectively used for indicating letters or numerical figures for inputting said second identification information, and wherein the input locations corresponding to individual ones of the letters or numerical figures are variable, such that individual ones of the letters or numerical figures are resident at one of the plurality of input locations when said second identification information is input a first time, and are resident at another of the plurality of input locations when said second identification information is input a second time.

44. (Previously Presented) The portable card terminal according to claim 43, wherein the plurality of input locations are varied prior to the inputting of said second identification information.

45. (Previously Presented) The portable card terminal according to claim 37, wherein said operating means includes a display unit for displaying letters and a selection unit for selecting the letters displayed in said display unit, and wherein the second identification

information input by said operating means is made up by a string of letters selected in said

selection unit from among plural letters sequentially displayed on said display unit.

46. (Previously Presented) An authentication system made up by a portable card

terminal and an authentication device provided independently of said portable card terminal for

communication with said portable card terminal, said authentication system comprising:

said portable card terminal, including

first identification information storage means having a first identification information

stored therein for discriminating said portable card terminal, said first identification information

comprising a portable card terminal identifier that uniquely identifies the portable card terminal,

operating means including display means for irregularly displaying letters included in a

group of letters and selection means for selecting the letters making up a second identification

information from among the letters irregularly displayed on said display means, said operating

means inputting the second identification information associated with said first identification

information,

encryption means for encrypting the second identification information input by said

operating means based on an encryption key information, and

first communication means for communication with said authentication device, wherein

said communication includes transmitting the first identification information to said

authentication device and receiving said encryption key information from the authentication

device in response to transmitting the first identification information;

said authentication device, including

second identification information storage means having the first identification

information and the second identification information stored therein,

encryption key information generating means for generating said encryption key information, wherein said encryption key information is generated in response to receiving the first identification information from said portable terminal,

second communication means for communication with said portable card terminal, and

comparator authentication means for comparing the second identification information encrypted by said encryption means to the second identification information stored in the second identification information storage means; wherein

said portable card terminal encrypts the second identification information input from said operating means, based on said encryption key information received from said authentication device through said first communication means, and the so-encrypted second identification information is transmitted through said first communication means to said authentication device; and

wherein, in said authentication device, the encrypted second identification information received through said second communication means and the second identification information stored by said second identification information storage means are compared to each other based on said encryption key information to perform the authentication.

APPENDIX B – ADDITIONAL EVIDENCE

None.

APPENDIX C – RELATED PROCEEDINGS

None.